NHS
Frimley
Clinical Commissioning Group

FRIMLEY
CLINICAL COMMISSIONING GROUP

Records Management Policy

Policy number	[Tbc by Governance team]
Version	Version 1.0
Approved by	Audit Committee in Common
Document Author	South Central West CSU
Date of approval	17 March 2021
Next due for review	1 April 2023

Version	Date	Author	Status	Comment
1.0	16/2/2021	SCW CSU	Draft	Version adapted from East Berkshire CCG version

Equality Statement

Frimley Clinical Commissioning Group (CCG) aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

Throughout the development of the policies and processes cited in this document, the CCG has:

- Given due regard to the need to eliminate discrimination, harassment and victimisation, to advance equality of opportunity, and to foster good relations between people who have shared a relevant protected characteristic (as cited under the Equality Act 2010) and those who do not share it;

- Given regard to the need to reduce inequalities between patients in access to, and outcomes from, healthcare services and in securing that services are provided in an integrated way where this might reduce health inequalities.

Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the member of staff has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

The CCG embraces the four staff pledges in the NHS Constitution. This policy is consistent with these pledges.

Contents

1. INTRODUCTION

This policy sets out how Frimley CCG (herein after referred to as '*CCG*') will approach the management of its records. This policy is part of a Records Management Framework that includes additional procedure, guidance, training, audit and strategy. Our records framework fits into the wider context of Information Governance.

All NHS records (including email and electronic documents) are public records under the terms of the Public Records Act 1958 sections 3(1)-(2), and must be kept in accordance with the following statutory and NHS guidelines:

- The Public Records Act 1958 and 1967
- The General Data Protection Regulations
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- Records Management Code of Practice for Health and Social Care 2016
- The Common Law Duty of Confidentiality
- Confidentiality: NHS Code of Practice
- NHS Information Governance: Guidance on Legal and Professional Obligations

Guidance on the management of NHS records is provided by the Department of Health. The Records Management: NHS code of Practice 2016 which sets out a schedule of minimum retention periods for many types of record and is based on legal requirements and professional best practice.

2. SCOPE AND DEFINITIONS

This policy covers all *CCG* business areas and all information, irrelevant of the media being used to store the information. Corporate records in all formats (paper and electronic), active and inactive, held for use in the organisation, including:

Administrative (e.g. corporate, provider services, contracts and commissioning, personnel, estates, finance and accounting, customer services and litigation) including e-mails, other communication tools and text messages

Records management is the process by which an organisation manages all the aspects of records and information, from their creation through to their eventual disposal (Records Lifecycle). The aim of the policy is to ensure:

- **Accountability** – Records are adequate to account fully and transparently for all business actions and decisions, in particular to:
  - protect legal and other rights of staff or those affected by those actions;
  - facilitate audit or examination;
  - provide credible and authoritative evidence.

- **Accessibility** – Records can be located when needed and only those with a legitimate right can access the records and the information within them is displayed in a way consistent with its initial use, and the current version is identified where multiple versions exist.

- **Interpretation** - The context of the record can be interpreted i.e. identification of staff who created or added to the record and when, during which business process, and were appropriate, how the record is related to other records.

- **Quality** – Records can be trusted - are complete and accurate and reliably represent the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.

- **Maintenance through time** - so that the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format.

- **Security** – Records are secure from unauthorised or inadvertent alteration or erasure, access and disclosure are properly controlled and there are audit trails to track all use and changes in order to ensure that records are held in a robust format which remains readable for as long as records are required.

- **Retention and disposal** – Records are retained and disposed of appropriately, using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value. The British Security Industry Association standard (BSIA) EN15713:2009 - Secure Destruction of Confidential Material must be adhered to when destroying confidential information

- **Staff are trained** – so that all staff are made aware of their responsibilities regarding records management.

3. PROCESSES/REQUIREMENTS

The CCG where applicable, its legacy organisations and records are its corporate memory, providing evidence to actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making and protect the interests of the CCG. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

The CCG operates within an Information Governance compliance environment. Failure to meet any relevant requirement could result in official sanction, reputation damage and even limits on what data and services we could provide as a business. The CCG must be compliant with the NHS Information Governance Toolkit Data Security and Protection Toolkit (DSPT) and Records Management Code of Practice for Health and Social Care 2016.

The organisational benefits from good records management are:

- control and availability of valuable information assets
- efficient use of staff time
- compliance with legislation and standards
- good utilisation of storage and server space
- a reduction in costs
- support the day to day business that underpins the delivery of a high quality service to our customers
- maintain the integrity of the records
- meet legal requirements
- monitoring and audit cycles

The CCG will establish and maintain policies to ensure compliance with the Records Management Code of Practice Health and Social Care 2016.

3.1 Records Management – Components and Principles

The International Organisation for Standardisation (ISO) 15489-1:2016 Information and documentation - Records management Records Lifecycle – defines a record as ‘information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of businesses. (Source: Records Management Code of Practice for Health and Social Care 2016).

Records Life Cycle	
Lifecycle Stage	**Description**
1. Planning	At a corporate level we shall develop and implement policy, procedures and functionality to deliver compliant records management strategy Our departments shall ensure they have identified key records that must be captured as a result of their activities and that these are managed following policy.
2. Creation & receipt	This is where a record is created and is saved. We shall ensure that our records are properly captured into approved filing systems, that they are protected from unauthorised access or change, are assigned the correct data classifications and are named following an agreed standard.
4. Retention	We shall retain non-current and superseded records in our filing system to support ongoing business needs and compliance requirements. Our disposal schedules shall govern how long records are retained. Retained records shall continue to be protected and accessible, with storage facilities meeting appropriate standards.
5. Disposal	Our records shall not be retained indefinitely. At the end of the agreed retention periods, records shall be disposed of and a destruction certificate will be issued. In most cases this will mean controlled destruction; a small percentage of records may become be flagged for permanent retention and will be passed to the appropriate place of deposit (POD).

3.2 General Data Protection Regulations (GDPR)

Under the General Data Protection Regulations (GDPR) the definition of ‘data concerning health’ is ‘personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status’ (Article 4(15)

‘Personal Data’ is defined as: ‘any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’ (Article 4(1))

Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

There are various GDPR definitions relating to the management of information and records in a health environment. For example, under Article 4;

- **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **'restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;
- **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- **'data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

For information on categories of data and their assigned definition, please refer to Appendix 3b - Categories of data/information**.**

3.3 Information Quality

Our records are evidence of our activities: they may be required for litigation, governance, external audits, statutory enquiries, patient care and as a basis for decision making. Our records need to be:

- ✓ complete (in terms of having been captured in full)
- ✓ accurate (factually correct, legibly and assured as to the integrity of the record.)
- ✓ relevant (the degree to which the data meets current and potential user's needs)
- ✓ accessible (available when needed)
- ✓ timely (recorded and available as soon after the event as possible) alterations or annotations (must be clearly identifiable, traceable to the author and authorised by an appropriate Senior Manager).

Clinical records must be timely, accurate, concise and up to date accounts of the assessment and treatment of individual patients. Good clinical record keeping is an integral and vital part of professional practice and may come under scrutiny should any issues arise.

Department/Process managers shall also be clear on what records are required to sufficiently document business activities, and ensure that staff capture them following policy and procedure

3.4 Manual / Paper Records

In keeping with wider NHS agenda (NHS England Five Year Forward Plan), we shall endeavour to maintain records electronically where practicable. Original electronic records will be considered the 'primary version'. Printed copies of electronic records should be maintained only by exception and shall be appropriately destroyed at the earliest convenience.

Where it is practical to do so, we shall scan new or legacy paper records following our scanning guidance (this follows standard British Standard (BS) 10008 to protect legal admissibility of scanned paper records). In some cases it might be desirable to hold original ink signed records. This is permissible, although scanning such documents is preferable so long as the scanned version is legally admissible.

Paper copies of records must be kept secure and should be stored in an appropriate locked filing cabinet, office or designated records store on site, or in an approved off-site storage facility, so they are available and accessible to those who need them.

3.5 Records Inventory

We shall use the Information Asset Register's to monitor and understand what collections of records and information we hold and note each documents retention period. We shall work towards organising our records into a Records File Plan that lists our business activities, and the records that they create, in a systematic and organised way.

3.6 Disposal Schedules and Legal Holds

We shall not retain all of our records indefinitely. Disposal is the process that leads to records being destroyed or transferred elsewhere. It includes a

record of what happened so that we can clearly show that we do not have the information any longer.

Disposal of any records shall be held if they pertain to an existing / emerging legal matter or request for information – this is known as a Legal Hold. An inventory of the retained records and the reason for the extended period of retention must be maintained.

Our records shall be retained and disposed of following agreed disposal schedules and procedures that are based on the Records Management Code of Practice for Health and Social Care 2016 and business needs. Disposal shall always be carried out following confidentiality and sensitivity requirements, the CCG should not retain records of legacy NHS organisations.

Unilateral disposal of records, particularly if done contrary to disposal schedules or legal holds, is a serious breach of policy.

3.7 Accredited File Shares

Our electronic records shall be saved to our approved and governed file share and shall include sub-folders that assist with disposal management.

Where records contain personally identifiable data and special categories of personal data that are considered as personal data or hold commercially confidential information. It is a legal requirement that such data is stored securely. You must ensure such data is stored within the Secure drive and have the correct protective marker applied – please refer to the section 3.9 Security and Access.

As a general rule, original electronic records shall not be saved to ‘offline’ storage such as non-networked computer hard drives, USBs or optical media. In some circumstances e.g. anticipated limited network connection, staff may need to save copies of records to **encrypted** devices such as a USB memory stick. This is permissible if the IT Services Acceptable Use Policy is followed, and any new records / versions are saved to the approved storage location as soon as possible and subsequently deleted from the storage device.

NB: this paragraph may not be applicable Customer records shall be stored and organised in such a way that they are easily distinguishable from CCG information and can be easily transferred to the customer if required.

3.8 Naming Electronic Documents

Record naming is an important process in records management and it is essential that a unified approach is undertaken within all areas of the CCG to aid in the management of records.

In constructing a title it is necessary to decide how best to describe the content of the file or the individual document. The most commonly used elements in the creation of a title are listed below. It will depend on the nature of the document or folder which elements will be the most suitable for use in the title.

Common elements of a title:

- Directorate name
- Date (if applicable)
- Subject
- Document status
- Version number

Staff members should refrain from naming folders or files with their own name unless the folder or file contains records that are biographical in nature about that individual, for example, personnel records.

3.9 Security and Access

Classification of NHS Information - Marking Guidance from NHS England

All information the CCG collects, stores, processes, generates or shares to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection.

Everyone who works within the CCG (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any CCG information or data that they access, irrespective of whether it is marked or not.

Access to staff records (electronically and/or hard copies) - these are kept secure with restricted access by the Corporate Services Manager and Head of Corporate Affairs. Line Managers can request access to these files if they need information from the file to manage performance issues and or need personal contact details.

Please refer to Appendix 3: Protective Marking Scheme for further information.

3.10 Line of business systems / databases

Many of our records are held within databases. These may be in the form of uploaded documents e.g. a PDF or email, or as data streams, e-transactions and system actions. This policy applies to these records. System owners and project managers shall consider the requirements of this policy when implementing, procuring or using databases.

Electronic records that are uploaded to databases, e.g. an email into Datix, should be deleted from local systems, e.g. Inbox or File Share. It is bad practice to duplicate information across systems.

3.11 Data Backups

All of our data including electronic records are ‘backed-up’ to offline storage in accordance with the relevant Backup and Business Continuity Policy. It is vital that ‘rescued’ records are complete copies and are not changed in any way, this includes embedded metadata e.g. date created, data last modified.

Backups are within scope of statutory access to information requests and legal disclosure. Records deleted from user front-end storage, e.g. file shares, shall also be deleted from the back-up and shadow copies. Current back-up policy is that any iteration of electronic data is backed-up for one year before being overwritten / deleted. In short, records that have been deleted from front-end systems within the last year may still be available in the back-up.

3.12 New Technologies – Cloud and Collaboration / Sharing

The use of new technologies to improve working practices, process monitoring and collaboration is becoming increasingly popular. These are characterised by services such as cloud storage and collaboration spaces being held outside of traditional on-site technology infrastructure.

The requirements of this policy shall apply to such technology because they are handling our information and records. Assurances must be in place to ensure that data retention schedules are meet and data is fully deleted, to include, back-up copies and ‘other’ structures that may refer to or directly reference the data, for example, a document index.

3.13 Email Records / Electronic Communication

Email is a key communication tool. The email service is designed as a communication tool and is not an appropriate solution for long term file storage. Therefore, all emails that are records of business activity and/or formal record of a transaction should be saved to an appropriately named folder on shared network drive. Keeping all emails will result in a significant storage burden to your organisation and information may become difficult to locate due to the size of files and attachments being stored.

NHS Mailboxes and Mailbox Archives should not be used for the long term storage of email records.

Particular attention must be paid to ensuring that emails relating to patients (clinical records) are dealt with promptly and where appropriate, deleted once the pertinent information has been transferred to the relevant record.

Staff shall regularly housekeep their Mailboxes so that transitory and spam type emails are disposed of. Managers shall ensure all required email records are transferred from a staff leaver's Mailbox to the approved store. Other forms of electronic communication such as Instant Messaging, voice recording and video conferencing will likely become more commonplace. These 'recordings', if retained, shall be managed under this policy.

3.14 Long Term Access and Protection – Record Preservation

We shall take steps to ensure that our records remain accessible and are not damaged during their retention; for some records this could be many decades. Such lengths of time require preservation management.

Our records shall be protected from unauthorised access and natural risks such as flooding and fire. A risk assessment of all storage solutions (on or off-site) must be undertaken to ensure the area meets the required structural and environmental standards, for example, IGTK standard – 14-301. Electronic records are at a particular risk of digital obsolescence and degradation of media. We shall undertake precautions to ensure the long term accessibility of electronic content including: using ubiquitous and open formats e.g. PDF, DOCx; regular refreshing and error-checking of storage media; maintaining all records on networked and backed-up drives rather than removable media storage e.g. CDs, USBs; and assessing the digital preservation risks of any new system.

4. ROLES AND RESPONSIBILITIES

Position or group	Description of Records Management Responsibility
Managing Director	Accountable for the proper and compliant conduct of records management across the organisation.
Caldicott Guardian and Executive Team	The Caldicott Guardian is Responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. They will support work to enable information sharing where it is appropriate to share, and advice on possible choices for meeting compliance when processing information. Executive Team cascade requirements of the policy to respective departments and support its implementation.
Data Protection Officer	The Data Protection Officer (DPO) has the responsibilities as set out in the GDPR guidance. The DPO will ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects the ICO (Information Commissioner's Office) is informed no later than 72 hours after the organisation becomes aware of the incident. They will also have a key role and be part of the Data Protection Impact Assessment process on behalf of the CCG.
Senior Information Risk Owner (SIRO)	Take ownership of the organisation's information risk policy. Acts as advocate for information risk on the board. Drive culture change with regard to information risks in a realistic and effective manner. Is advised and supported by the Information Governance Steering Group (IGSG).
CCG **Records Manager**	Day-to-day operational management of the records management programme and framework. Drafting policy and procedures. Conducting audits. Supporting and training staff. Providing records management services to customers.
Information Asset Owners (IAO)	The SIRO is supported by Information Asset Owners (IAOs). The role of the IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. The Information Governance Team will support the IAOs in fulfilling their role.
Data Custodians (DCs)	Data Custodians are required to support the IAO's and the CCG SIRO who will work with the Information Governance Team to ensure staff apply the Data Protection Legislation and Caldicott

	Principles within working practices. The Information Governance Team will provide local face to face IG training if required and will monitor staff compliance by way of the consult OD portal and link to the e-LfH platform.
Department / Process managers	Ensure records produced by their respective activities are identified and captured following policy. Ensure that staff have attended required record keeping training. Work with local IG and records roles.
All staff	All staff, and those working on behalf of the organisation, are expected to follow this policy and its procedures. All staff who create and use records as part of the delivery of the CCG business. This covers records in all formats (paper and electronic), both active and inactive

5. TRAINING

All staff are required to comply with the CCG IG Staff Handbook which stresses the importance of appropriate information handling which incorporates statutory, common law and best practice requirements. Information Governance is a framework drawing these requirements together; therefore it is important that staff receive the appropriate training.

The CCG will ensure all staff receive annual Information Governance training appropriate to their role through the online E-Learning for Health training tool or face to face training delivered by the CCG Information Governance Team. Managers are responsible for monitoring staff compliance. New starters and any temporary, contract or agency staff must also complete the annual Information Governance Training.

On joining the organisation, CCG staff will receive a copy of the Information Governance staff handbook and will be required to sign and return a receipt to the CCG IG Team.

6. PUBLIC SECTOR EQUALITY DUTY- EQUALITY IMPACT ASSESSMENT

The CCG aims to design and implement services, policies and measures that are fair and equitable. An equality analysis has been completed for this policy and no adverse impact was identified.

Should any adverse impact on equality be subsequently detected or highlighted by staff and other users of the policy then this will be analysed and remedial action taken as appropriate.

7. MONITORING COMPLIANCE AND EFFECTIVENESS

This policy will be monitored by the Information Governance Steering Group to ensure any legislative changes that occur before the review date are incorporated.

Our performance in records management compliance shall be audited following a scheduled plan using a defined audit methodology. Information Asset Owners will have direct responsibility for ensuring their information practices are audited with support from the Records Manager and Information Governance team. Where non-compliance or improvements could be made then these shall be agreed with process owners / managers and subsequently followed up.

This policy, along with its supporting procedures, shall be reviewed no later than two years after approval or earlier should there be significant changes to the regulatory environment or organisation.

Failure to comply with this policy may result in ineffective working and an inability to meet the requirements of the Freedom of Information and the General Data Protection Regulations 2018. Where the policy is breached, this must be reported via the CCG incident reporting process and the Data Protection Officer and Caldicott Guardian informed, if required.

8. REVIEW

In compliance with Data Security and Protection Toolkit requirements, this policy will be reviewed annually. The policy review will into account comments received from NHS South, Central and West Commissioning Support Unit, Corporate Governance & Assurance Group and will be viewed by the Senior Information Risk Owner, Caldicott Guardian, Deputy Data Protection Officer and Head of Information Governance.

9. REFERENCES AND ASSOCIATED DOCUMENTS

- Information Commissioners Office (Data Protection Act 2018 and General Data Protection Regulation) – www.ico.gov.uk/
- National Archives (Public Records) – www.nationalarchives.gov.uk

- Data Security and Protection Toolkit – https://www.dsptoolkit.nhs.uk
- NHS England (Document and Records Management Policy Final V3) - https://www.england.nhs.uk/
- Records Management Code of Practice for Health and Social Care 2016 - http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf
- Government Security Classifications April 2014 - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf
- CCG Information Governance Policy
- CCG Information Governance Management and Strategy Framework
- CCG Information Governance Handbook
- CCG Information Governance Confidentiality Policy
- CCG IT Services – Backup and Business Continuity Policy
- CCG Service Equipment Disposal Policy
- CCG Records Management associated procedures and guidance
- Guidance from legacy CCG organisations

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT

1.	**Title of policy/ programme/ framework/ strategy being analysed.**		
2.	**Please state the aims and objectives of the work and intended equality outcomes** *This policy forms part of the wider commitment across the NHS to be an employer of choice and recognises that there are significant advantages in terms of employee recruitment, motivation and retention, where flexible working arrangements are offered in conjunction with a commitment to service to patients.*		
3.	**Who is likely to be affected? Eg staff, patients, service users, carers**		
4.	**What evidence do you have of potential impact (positive and negative)**		
		Yes/No	**Comments**
1.	**Does the document/guidance affect one group less or more favourably than another on the basis of:**		
	• Race		
	• Ethnic origins (including gypsies and travellers)		
	• Nationality		
	• Gender		
	• Culture		
	• Religion or belief		
	• Sexual orientation including lesbian, gay and bisexual people		
	• Age		
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems		

2.	**Is there any evidence that some groups are affected differently?**		
3.	**If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?**		
4.	**Is the impact of the document/guidance likely to be negative?**		
5.	**If so, can the impact be avoided?**		
6.	**What alternative is there to achieving the document/guidance without the impact?**		
7.	**Can we reduce the impact by taking different action?**		

Who	Date of Assessments

APPENDIX 2 - KEY RECORDS MANAGEMENT REQUIREMENTS

Legislation / Standard	Compliance Requirement
Public Records Act 1958	All NHS records are Public Records. All NHS organisations must make arrangements for the safe keeping and disposal of their information and records. Recent changes have reduced the 30 year public records disposal rule to 20 years.
Freedom of Information Act 2000 including Section 46 Code of Practice for Records Management.	Provisions for disclosure of information held by public authorities. Includes a Records Management Code of Practice to support the Act which gives guidance on good practice in records management. It applies to all authorities subject to the Act, to the Public Records Act 1958 or to the Public Records Act (Northern Ireland) 1923.
General Data Protection Regulations	Regulates the processing of personal data relating to living persons. Article 5 of the GDPR requires that personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to individuals; b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the

	appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.”
Data Protection Act 2018 (DPA 2018)	The Data Protection Act 2018 replaces the Data Protection Act 1998 and legislates to an equivalent to the GDPR but includes national derogations not covered by the GDPR. The DPA 2018 should be read in conjunction with the GDPR.
Access to Health Records Act 1990	Regulates access to the records of a deceased person.
Records Management Code of Practice for Health and Social Care 2016	The guidelines in this Code apply to NHS records, including records of NHS patients treated on behalf of the NHS in the private healthcare sector and public health records, regardless of the media on which they are held. The code includes records of staff, complaints, corporate records and any other records held in any format or media.

APPENDIX 3 - CLINICAL RECORDS GUIDANCE

GDPR Recital number 35 clarifies that Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes:

- information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person;
- a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes;
- information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples;
- information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

Good clinical record keeping is an integral and vital part of professional practice which contributes to a high standard of:

- The delivery of clinical care
- Continuity of care
- The sharing of information and improving communication between parties
- Business and reporting purposes

Clinical records must be timely, accurate, concise and up to date account of the assessment and treatment of individual patients.

SomeCCG business activities will create or receive clinical records. Information held in these records will relate to any aspect of patient health, treatment and other care they receive and, by their nature, are considered as OFFICIAL-SENSITIVE: PERSONAL.

Only business areas that specifically require clinical records to carry out their work should have access to them. If you receive clinical records and you are not sure why then report this to your Manager and (relevant IG contact in

The Team or individual employees are responsible for the safeguarding of confidential information held as paper records (in a structured filing system) and electronically (on computers and within an agreed filing procedure). Please ensure there are robust ‘track and trace’ mechanisms place for all paper records, e.g. tracer cards and access to electronic information must be appropriately restricted.

Unavailable, mislaid or lost clinical records are a serious risk and immediate action must be taken. The appropriate Department must log this as an incident on DATIX and carry out an investigation

Any unauthorised use of clinical information, e.g. searching for information about a relative or any use of information outside of a “legitimate professional relationship” may lead to immediate disciplinary action. This would be viewed as a breach of confidentiality.

APPENDIX 4 - PROTECTIVE MARKING SCHEME

Classification of NHS Information - Marking Guidance from NHS England
The new Government Security Classifications levels are;

OFFICIAL

Definition – ALL routine public sector business, operations and services should be treated as OFFICIAL. The CCG will operate exclusively at this level including the subset categories of OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL–SENSITIVE: PERSONAL where applicable. See Table 1 for examples.

SECRET

Definition – Very sensitive government (or partners) information that requires protection against the highly capable threats, such as well-resourced and determined threat actors and highly serious organised crime groups.

TOP SECRET

Definition – Exceptionally sensitive Government (or partners) information assets that directly support (or threaten) the national security of the UK or allies and requires extremely high assurance or protection against highly bespoke and targeted attacks.

Please note, there is no need to apply the new classification procedure retrospectively.
This simplified procedure will make it easier and more efficient for information to be handled and protected. The new procedure places greater emphasis on individuals taking personal responsibility for data they handle.

All information used by the CCG is by definition 'OFFICIAL.' It is highly unlikely the CCG will work with 'SECRET' or 'TOP SECRET' information.
Things to remember about OFFICIAL information:

1. Ordinarily OFFICIAL information does not need to be marked for non-confidential information.

2. A limited subset of OFFICIAL information could have more damaging consequences if it were accessed by individuals by accident or on purpose, lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL classification tier, but should have additional measures applied in the form of OFFICIAL-SENSITIVE.

3. This marking is necessary for person-identifiable information and commercially sensitive information and is applicable to paper and electronic records.

4. In additional to the marking of OFFICIAL-SENSITIVE further detail is required due to the content of the document or record, i.e.:

OFFICIAL – SENSITIVE: COMMERCIAL
Definition - Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG or a commercial partner if improperly accessed.

Or

OFFICIAL – SENSITIVE: PERSONAL
Definition - Personal information relating to an identifiable individual where inappropriate access could have damaging consequences.

Such documents/records should be marked with the caveat 'OFFICIAL-SENSITIVE: COMMERICAL or SENSITIVE' in capitals at the **top and bottom** of the page.
In unusual circumstances OFFICIAL – SENSITIVE information may contain both Personal and Commercial data, in such cases the descriptor OFFICIAL – SENSITIVE will suffice.

<u>NHS Confidential</u>
In the interim, some NHS organisations may still work to existing IG guidance; consequently any information received from an NHS organisation may be marked as NHS Confidential which should then be treated as OFFICIAL – SENSITIVE depending on its type.

How to handle and store OFFICIAL information;
EVERYONE is responsible to handle OFFICIAL information with care by:

- Applying clear desk policy
- information sharing with the right people
- Taking extra care when sharing information with external partners i.e. send information to named recipients at known addresses
- Locking your screen before leaving the computer
- Using discretion when discussing information out of the office

How to handle and store OFFICIAL – SENSITIVE information;

All OFFICIAL-SENSITIVE material including documents, media and other material should be physically secured to prevent unauthorised access. As a minimum, when not in use, OFFICIAL-SENSITIVE:PERSONAL or OFFICIAL-SENSITIVE: COMMERCIAL material should be stored in a secure encrypted device such as a secure drive or encrypted data stick, lockable room, cabinets or drawers.

- Always apply appropriate protection and comply with the handling rules
- Always question whether your information may need stronger protection
- Make sure documents are not overlooked when working remotely or in public areas, work digitally to minimise the risk of leaving papers on trains, etc
- Only print sensitive information when absolutely necessary
- Send sensitive information by the secure email route or use encrypted data transfers
- Encrypt all sensitive information stored on removable media particularly where it is outside the organisation's physical control
- Store information securely when not in use and use a locked cabinet/drawer if paper is used
- If faxing the information, make sure the recipient is expecting your fax and double check their fax number
- Take extra care to be discreet when discussing sensitive issues by telephone, especially when in public areas and minimise sensitive details
- Only in exceptional cases, where a business need if identified, should sensitive information be emailed over the internet, in an encrypted format, to the third parties. Contact the Corporate IG team for further advice
- The use of pin code for secure printing is both widely available and preferable way to manage the printing process

There is no need to apply the new classification procedure retrospectively.

Our Accredited File Shares shall include protected folders and permission protocols where OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL–SENSITIVE: PERSONAL information is held. Access to OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL–SENSITIVE: PERSONAL paper files should be restricted and monitored thus ensuring adequate security measures are in place. NB: All paper records must be tracked to ensure their exact location is known at all times.

Access restrictions to records shall be proportionate. Wherever possible, records and information should be available to all staff to aid information sharing, and reduce duplication and data volumes. Although clinical records must be kept secure on a need-to-know basis, this does not mean that they cannot be made available in a timely fashion to those who justifiably need access.

Example descriptors that may be used with OFFICIAL-SENSITIVE: COMMERCIAL OR OFFICIAL-SENSITIVE: PERSONAL and respective category of data/information as detailed in Appendix 3b.		
Category /data type	**Definition**	**Marking**
Appointments (Commercially confidential information)	Concerning actual or potential appointments not yet announced	OFFICIAL-SENSITIVE: COMMERCIAL
Barred (Personal Confidential Data)	Where there is a statutory (Act of Parliament or European Law) prohibition on disclosure, or disclosure would constitute a contempt of Court (information the subject of a court order)	OFFICIAL-SENSITIVE: COMMERCIAL
Board (Commercially Confidential Data)	Documents for consideration by an organisation's Board of Directors, initially, in private (Note: This category is not appropriate to a document that could be categorised in some other way)	OFFICIAL-SENSITIVE: COMMERCIAL
Commercial (Commercially Confidential Information)	Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs	OFFICIAL-SENSITIVE: COMMERCIAL
Contracts (Commercially Confidential Information)	Concerning tenders under consideration and the terms of tenders accepted	OFFICIAL-SENSITIVE: COMMERCIAL

For Publication (Commercially Confidential Information)	Where it is planned that the information in the completed document will be published at a future (even if not yet determined) date	OFFICIAL-SENSITIVE: COMMERCIAL
Management (Commercially Confidential Information)	Concerning policy and planning affecting the interests of groups of staff (Note: Likely to be exempt only in respect of some health and safety issues)	OFFICIAL-SENSITIVE: COMMERCIAL
Patient Information (to include Personal Confidential Data, Personal Data and 'Special Categories' of Personal Data)	Concerning identifiable information about patients	OFFICIAL-SENSITIVE: PERSONAL
Personal (to include Personal Confidential Data, Personal Data and 'Special Categories' of Personal Data)	Concerning matters personal to the sender and/or recipient	OFFICIAL-SENSITIVE: PERSONAL
Policy (Commercially Confidential Information)	Issues of approach or direction on which the organisation needs to take a decision (often information that will later be published)	OFFICIAL-SENSITIVE: COMMERCIAL
Proceedings (Commercially Confidential Information)	Corporate information is (or may become) the subject of, or concerned in a legal action or investigation.	OFFICIAL-SENSITIVE: COMMERCIAL
Staff (to include Personal Confidential Data, Personal Data and 'Special Categories' of Personal Data)	Concerning identifiable information about staff to include investigations, disciplinary hearings and grievances.	OFFICIAL-SENSITIVE: PERSONAL

APPENDIX 5 - CATEGORIES OF DATA/INFORMATION

Please note that the categories of data/information listed below, will be used or referred to in all CCG Polices. The purpose of this approach is to ensure a consistent approach is adopted.	
Personal Data (derived from the GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (derived from the GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

APPENDIX 6 – RECORDS MANAGEMENT RETENTION SCHEDULE

Please note that the CCG retention approach will be the same approach that is detailed in the NHS Records Management Code of Practice for Health & Social Care 2016 detailed **here**.

Broad descriptor	Record Type	Retention Start	Retention period	Action at end of retention period	Notes
Care Records with standard retention periods	Adult health records not covered by any other section in this schedule	Discharge or patient last seen	8 years	Review and if no longer needed destroy	Basic health and social care retention period - check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.
Care Records with standard retention periods	Adult social care records	End of care or client last seen	8 years	Review and if no longer needed destroy	
Care Records with standard retention periods	Children's records including midwifery, health visiting and school nursing	Discharge or patient last seen	25th or 26th birthday (see Notes)	Review and if no longer needed destroy	Basic health and social care retention requirement is to retain until 25th birthday or if the patient was 17 at the conclusion of the treatment, until their 26th birthday. Check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.

Care Records with standard retention periods	Electronic Patient Records System	See Notes	See Notes	Destroy	Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed. If the system does not have this capacity, then once the records have reached the end of their retention periods they should be inaccessible to users of the system and upon decommissioning, the system (along with audit trails) should be retained for the retention period of the last entry related to the schedule.
Care Records with standard retention periods	General Dental Services records	Discharge or patient last seen	10 Years	Review and if no longer needed destroy	
Care Records with standard retention periods	GP Patient records	Death of Patient	10 years after death see Notes for exceptions	Review and if no longer needed destroy	If a new provider requests the records, these are transferred to the new provider to continue care. If no request to transfer: 1. Where the patient does not come back to the practice and the records are not transferred to a new provider the record must be retained for 100 years unless it is known that they have emigrated 2. Where a patient is known to have emigrated, records may be reviewed and destroyed after 10 years 3. If the patient comes back within the 100 years, the retention reverts to 10 years after death.

Care Records with standard retention periods	Mental Health records	Discharge or patient last seen	20 years or 8 years after the patient has died	Review and if no longer needed destroy	Covers records made where the person has been cared for under the Mental Health Act 1983 as amended by the Mental Health Act 2007. This includes psychology records. Retention solely for any persons who have been sectioned under the Mental Health Act 1983 must be considerably longer than 20 years where the case may be ongoing. Very mild forms of adult mental health treated in a community setting where a full recovery is made may consider treating as an adult records and keep for 8 years after discharge. All must be reviewed prior to destruction taking into account any serious incident retentions.
Care Records with standard retention periods	Obstetric records, maternity records and antenatal and post natal records	Discharge or patient last seen	25 years	Review and if no longer needed destroy	For the purposes of record keeping these records are to be considered as much a record of the child as that of the mother.
Care Records with Non-Standard Retention Periods	Cancer/Oncology - the oncology records of any patient	Diagnosis of Cancer	30 Years or 8 years after the patient has died	Review and consider transfer to a Place of Deposit	For the purposes of clinical care the diagnosis records of any cancer must be retained in case of future reoccurrence. Where the oncology records are in a main patient file the entire file must be retained. Retention is applicable to primary acute patient record of the cancer diagnosis and treatment only. If this is part of a wider patient record then the entire record may be retained. Any oncology records must be reviewed prior to destruction taking into account any potential long term research value which may require consent or anonymisation of the record.

Care Records with Non-Standard Retention Periods	Contraception, sexual health, Family Planning and Genito-Urinary Medicine (GUM)	Discharge or patient last seen	8 or 10 years (see Notes)	Review and if no longer needed destroy	Basic retention requirement is 8 years unless there is an implant or device inserted, in which case it is 10 years. All must be reviewed prior to destruction taking into account any serious incident retentions. If this is a record of a child, treat as a child record as above.
Care Records with Non-Standard Retention Periods	HFEA records of treatment provided in licenced treatment centres		3, 10, 30, or 50 years	Review and if no longer needed destroy	Retention periods are set out in the HFEA guidance at:http://www.hfea.gov.uk/docs/General_directions_0012.pdf
Care Records with Non-Standard Retention Periods	Medical record of a patient with Creutzfeldt-Jakob Disease (CJD)	Diagnosis	30 Years or 8 years after the patient has died	Review and consider transfer to a Place of Deposit	For the purposes of clinical care the diagnosis records of CJD must be retained. Where the CJD records are in a main patient file the entire file must be retained. All must be reviewed prior to destruction taking into account any serious incident retentions.
Care Records with Non-Standard Retention Periods	Record of long term illness or an illness that may reoccur	Discharge or patient last seen	30 Years or 8 years after the patient has died	Review and if no longer needed destroy	Necessary for continuity of clinical care.The primary record of the illness and course of treatment must be kept of a patient where the illness may reoccur or is a life long illness.

Pharmacy	Information relating to controlled drugs	Creation	See Notes	Review and if no longer needed destroy	NHS England and NHS BSA guidance for controlled drugs can be found at: http://www.nhsbsa.nhs.uk/PrescriptionServices/1120.aspx and https://www.england.nhs.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf The Medicines, Ethics and Practice (MEP) guidance can be found at the link (subscription required) http://www.rpharms.com/support/mep.asp#new Guidance from NHS England is that locally held controlled drugs information should be retained for 7 years. NHS BSA will hold primary data for 20 years and then review.NHS East and South East Specialist Pharmacy Services have prepared pharmacy records guidance including a specialised retention schedule for pharmacy. Please see:http://www.medicinesresources.nhs.uk/en/Communities/NHS/SPS-E-and-SE-England/Reports-Bulletins/Retention-of-pharmacy-records/

Pharmacy	Pharmacy prescription records *see also Controlled Drugs*	Discharge or patient last seen	2 Years	Review and if no longer needed destroy	See also 'Controlled Drugs'. There will also be an entry in the patient record and a record held by the NHS Business Services Authority. NHS East and South East Specialist Pharmacy Services have prepared pharmacy records guidance including a specialised retention schedule for pharmacy. Please see: http://www.medicinesresources.nhs.uk/en/Communities/NHS/SPS-E-and-SE-England/Reports-Bulletins/Retention-of-pharmacy-records/

Pathology	Pathology Reports/Information about Specimens and samples	Specimen or sample is destroyed	See Notes	Review and consider transfer to a Place of Deposit	This Code is concerned with the information about a specimen or sample. The length of storage of the clinical material will drive the length of time the information about it is to be kept. For more details please see: https://www.rcpath.org/resourceLibrary/the-retention-and-storage-of-pathological-records-and-specimens--5th-edition-.html. Retention of samples for clinical purposes can be for as long as there is a clinical need to hold the specimen or sample. Reports should be stored on the patient file. It is common for pathologists to hold duplicate reports. For clinical purposes this is 8 years after the patient is discharged for an adult or until a child's 25th birthday whichever is the longer. . After 20 years for adult records there must be an appraisal as to the historical importance of the information and a decision made as to whether they should be destroyed of kept for archival value.
Event & Transaction Records	Blood bank register	Creation	30 Years minimum	Review and consider transfer to a Place of Deposit	
Event & Transaction Records	Clinical Audit	Creation	5 years	Review and if no longer	

				needed destroy	
Event & Transaction Records	Chaplaincy records	Creation	2 years	Review and consider transfer to a Place of Deposit	See also Corporate Retention
Event & Transaction Records	Clinical Diaries	End of the year to which they relate	2 years	Review and if no longer needed destroy	Diaries of clinical activity & visits must be written up and transferred to the main patient file. If the information is not transferred the diary must be kept for 8 years.
Event & Transaction Records	Clinical Protocols	Creation	25 years	Review and consider transfer to a Place of Deposit	Clinical protocols may have archival value. They may also be routinely captured in clinical governance meetings which may form part of the permanent record (see Corporate Records).
Event & Transaction Records	Datasets released by HSCIC under a data sharing agreement	Date specified in the data sharing agreement	Delete with immediate effect	Delete according to HSCIC instruction	http://www.hscic.gov.uk/media/15729/DARS-Data-Sharing-Agreement/pdf/Data_Sharing_Agreement_2015v2%28restricted_editing%29.pdf

Event & Transaction Records	Destruction Certificates or Electronic Metadata destruction stub or record of clinical information held on destroyed physical media	Destruction of record or information	20 Years	Review and consider transfer to a Place of Deposit	Destruction certificates created by public bodies are not covered by an instrument of retention and if a Place of Deposit or the National Archives do not class them as a record of archival importance they are to be destroyed after 20 years.
Event & Transaction Records	Equipment maintenance logs	Decommissioning of the equipment	11 years	Review and consider transfer to a Place of Deposit	
Event & Transaction Records	General Ophthalmic Services patient records related to NHS financial transactions	Discharge or patient last seen	6 Years	Review and if no longer needed destroy	
Event & Transaction Records	GP temporary resident forms	After treatment	2 years	Review and if no longer needed destroy	Assumes a copy sent to responsible GP for inclusion in the primary care record

Event & Transaction Records	Inspection of equipment records	Decommissioning of equipment	11 Years	Review and if no longer needed destroy	
Event & Transaction Records	Notifiable disease book	Creation	6 years	Review and if no longer needed destroy	
Event & Transaction Records	Operating theatre records	End of year to which they relate	10 Years	Review and consider transfer to a Place of Deposit	If transferred to a place of deposit the duty of confidence continues to apply and can only be used for research if the patient has consented or the record is anonymised.
Event & Transaction Records	Patient Property Books	End of the year to which they relate	2 years	Review and if no longer needed destroy	
Event & Transaction Records	Referrals not accepted	Date of rejection.	2 years as an ephemeral record	Review and if no longer needed destroy	The rejected referral to the service should also be kept on the originating service file.
Event & Transaction Records	Requests for funding for care not accepted	Date of rejection	2 years as an ephemeral record	Review and if no longer needed destroy	

Event & Transaction Records	Screening, including cervical screening, information where no cancer/illness detected is detected	Creation	10 years	Review and if no longer needed destroy	Where cancer is detected see 2 Cancer / Oncology. For child screening treat as a child health record and retain until 25th birthday or 10 years after the child has been screened whichever is the longer.
Event & Transaction Records	Smoking cessation	Closure of 12 week quit period	2 years	Review and if no longer needed destroy	
Event & Transaction Records	Transplantation Records	Creation	30 Years	Review and consider transfer to a Place of Deposit	See guidance at: https://www.hta.gov.uk/codes-practice
Event & Transaction Records	Ward handover sheet	Date of handover	2 years	Review and if no longer needed destroy	This retention relates to the ward. The individual sheets held by staff must be destroyed confidentially at the end of the shift.

Telephony Systems & Services (999 phone numbers,111 phone numbers, ambulance, out of hours, single point of contact call centres).	Recorded conversation which may later be needed for clinical negligence purpose	Creation	3 Years	Review and if no longer needed destroy	The period of time cited by the NHS Litigation Authority is 3 years
Telephony Systems & Services (999 phone numbers,111 phone numbers, ambulance, out of hours, single point of contact call centres).	Recorded conversation which forms part of the health record	Creation	Store as a health record	Review and if no longer needed destroy	It is advisable to transfer any relevant information into the main record through transcription or summarisation. Call handlers may perform this task as part of the call. Where it is not possible to transfer clinical information from the recording to the record the recording must be considered as part of the record and be retained accordingly.

Telephony Systems & Services (999 phone numbers,111 phone numbers, ambulance, out of hours, single point of contact call centres).	The telephony systems record(not recorded conversations)	Creation	1 year	Review and if no longer needed destroy	This is the absolute minimum specified to meet the NHS contractual requirement.
Births, Deaths & Adoption Records	Birth Notification to Child Health	Receipt by Child health department	25 years	Review and if no longer needed destroy	Treat as a part of the child's health record if not already stored within health record such as the health visiting record.
Births, Deaths & Adoption Records	Birth Registers	Creation	2 years	Review and actively consider transfer to a Place of Deposit	Where registers of all the births that have taken place in a particular hospital/birth centre exist, these will have archival value and should be retained for 25 years and offered to a Place of Deposit at the end of this retention period. Information is also held in the NHS Number for Babies (NN4B) electronic system and by the Office for National Statistics. Other information about a birth must be recorded in the care record.

Births, Deaths & Adoption Records	Body Release Forms	Creation	2 years	Review and consider transfer to a Place of Deposit	
Births, Deaths & Adoption Records	Death - cause of death certificate counterfoil	Creation	2 years	Review and consider transfer to a Place of Deposit	
Births, Deaths & Adoption Records	Death register information sent to General Registry Office on monthly basis	Creation	2 years	Review and consider transfer to a Place of Deposit	A full dataset is available from the Office for National Statistics.
Births, Deaths & Adoption Records	Local Authority Adoption Record (normally held by the Local Authority children's services)	Creation	100 years from the date of the adoption order	Review and consider transfer to a Place of Deposit	The primary record of the adoption process is held by the local authority children's service responsible for the adoption service
Births, Deaths & Adoption Records	Mortuary Records of deceased	End of year to which they relate	10 Years	Review and consider transfer to a Place of Deposit	

Births, Deaths & Adoption Records	Mortuary register	Creation	10 Years	Review and consider transfer to a Place of Deposit	
Births, Deaths & Adoption Records	NHS Medicals for Adoption Records	Creation	8 years or 25th birthday	Review and consider transfer to a Place of Deposit	The health reports will feed into the primary record held by Local Authority Children's services. This means that the adoption records held in the NHS relate to reports that are already kept in another file which is kept for 100 years by the appropriate agency and local authority.
Births, Deaths & Adoption Records	Post Mortem Records	Creation	10 years	Review and if no longer needed destroy	The primary post mortem file will be maintained by the coroner. The coroner will retain the post mortem file including the report. Local records of post mortem will not need to be kept for the same extended time.
Clinical Trials & Research	Advanced Medical Therapy Research Master File	Closure of research	30 years	Review and consider transfer to a Place of Deposit	See guidance at: https://www.gov.uk/guidance/advanced-therapy-medicinal-products-regulation-and-licensing For clinical trials record retention please see the MHRC guidance at https://www.gov.uk/guidance/good-clinical-practice-for-clinical-trials
Clinical Trials & Research	Clinical Trials Master File of a trial authorised under the	Closure of trial	25 years	Review and consider transfer to a	For details see: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.158.01.0001.01.ENG

	European portal under Regulation (EU) No 536/2014			Place of Deposit	
Clinical Trials & Research	European Commission Authorisation (certificate or letter) to enable marketing and sale within the EU member states area	Closure of trial	15 years	Review and consider transfer to a Place of Deposit	http://ec.europa.eu/health/files/eudralex/vol-2/a/vol2a_chap1_2013-06_en.pdf
Clinical Trials & Research	Research data sets	End of research	Not more than 20 years	Review and consider transfer to a Place of Deposit	http://tools.jiscinfonet.ac.uk/downloads/bcs-rrs/managing-research-records.pdf

Clinical Trials & Research	Research Ethics Committee's documentation for research proposal	End of research	5 years	Review and consider transfer to a Place of Deposit	For details please see:http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/ Data must be held for sufficient time to allow any questions about the research to be answered. Depending on the type of research the data may not need to be kept once the purpose has expired. For example data used for passing an academic exam may be destroyed once the exam has been passed and there is no further academic need to hold the data. For more significant research a place of deposit may be interested in holding the research. It is best practice to consider this at the outset of research and orphaned personal data can inadvertently cause a data breach.
Clinical Trials & Research	Research Ethics Committee's minutes and papers	Year to which they relate	Before 20 years	Review and consider transfer to a Place of Deposit	Committee papers must be transferred to a place of deposit as a public record: http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/
Corporate Governance	Board Meetings	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	

Corporate Governance	Board Meetings (Closed Boards)	Creation	May retain for 20 years	Transfer to a Place of Deposit	Although they may contain confidential or sensitive material they are still a public record and must be transferred at 20 years with any FOI exemptions noted or duty of confidence indicated.
Corporate Governance	Chief Executive records	Creation	May retain for 20 years	Transfer to a Place of Deposit	This may include emails and correspondence where they are not already included in the board papers and they are considered to be of archival interest.
Corporate Governance	Committees Listed in the Scheme of Delegation or that report into the Board and major projects	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Corporate Governance	Committees/ Groups / Sub-committees not listed in the scheme of delegation	Creation	6 Years	Review and if no longer needed destroy	Includes minor meetings/projects and departmental business meetings

Corporate Governance	Destruction Certificates or Electronic Metadata destruction stub or record of information held on destroyed physical media	Destruction of record or information	20 Years	Consider Transfer to a Place of Deposit and if no longer needed to destroy	The Public Records Act 1958 limits the holding of records to 20 years unless there is an instrument issued by the Minister with responsibility for administering the Public Records Act 1958. If records are not excluded by such an instrument they must either be transferred to a place of deposit as a public record or destroyed 20 years after the record has been closed.
Corporate Governance	Incidents (serious)	Date of Incident	20 Years	Review and consider transfer to a Place of Deposit	
Corporate Governance	Incidents (not serious)	Date of Incident	10 Years	Review and if no longer needed destroy	
Corporate Governance	Non-Clinical Quality Assurance Records	End of year to which the assurance relates	12 years	Review and if no longer needed destroy	
Corporate Governance	Patient Advice and Liaison Service (PALS) records	Close of financial year	10 years	Review and if no longer needed destroy	

Corporate Governance	Policies, strategies and operating procedures including business plans	Creation	Life of organisation plus 6 years	Review and consider transfer to a Place of Deposit	
Communications	Intranet site	Creation	6 years	Review and consider transfer to a Place of Deposit	
Communications	Patient information leaflets	End of use	6 years	Review and consider transfer to a Place of Deposit	
Communications	Press releases and important internal communications	Release Date	6 years	Review and consider transfer to a Place of Deposit	Press releases may form a significant part of the public record of an organisation which may need to be retained
Communications	Public consultations	End of consultation	5 years	Review and consider transfer to a Place of Deposit	

Communications	Website	Creation	6 years	Review and consider transfer to a Place of Deposit	
Staff Records & Occupational Health	Duty Roster	Close of financial year	6 years	Review and if no longer needed destroy	
Staff Records & Occupational Health	Exposure Monitoring information	Monitoring ceases	40 years/5 years from the date of the last entry made in it	Review and if no longer needed destroy	A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any other case, for at least 5 years.
Staff Records & Occupational Health	Occupational Health Reports	Staff member leaves	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner	Review and if no longer needed destroy	

Staff Records & Occupational Health	Occupational Health Report of Staff member under health surveillance	Staff member leaves	Keep until 75th birthday	Review and if no longer needed destroy	
Staff Records & Occupational Health	Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses	Staff member leaves	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed destroy	
Staff Records & Occupational Health	Staff Record	Staff member leaves	Keep until 75th birthday (see Notes)	Create Staff Record Summary then review or destroy the main file.	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. May be destroyed 6 years after the staff member leaves or the 75th birthday, whichever is sooner, if a summary has been made.
Staff Records & Occupational Health	Staff Record Summary	6 years after the staff member leaves	75th Birthday	Place of Deposit should be offered for continued retention or Destroy	Please see page 36 for an example of a Staff Record Summary used by an organisation.

Staff Records & Occupational Health	Timesheets (original record)	Creation	2 years	Review and if no longer needed destroy	
Staff Records & Occupational Health	Staff Training records	Creation	See Notes	Review and consider transfer to a Place of Deposit	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The IGA recommends: 1 Clinical training records - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer2 Statutory and mandatory training records - to be kept for ten years after training completed3Other training records - keep for six years after training completed.
Procurement	Contracts sealed or unsealed	End of contract	6 years	Review and if no longer needed destroy	
Procurement	Contracts - financial approval files	End of contract	15 years	Review and if no longer needed destroy	
Procurement	Contracts - financial approved suppliers documentation	When supplier finishes work	11 years	Review and if no longer needed destroy	

Procurement	Tenders (successful)	End of contract	6 years	Review and if no longer needed destroy	
Procurement	Tenders (unsuccessful)	Award of tender	6 years	Review and if no longer needed destroy	
Estates	Building plans and records of major building work	Completion of work	Lifetime of the building or disposal of asset plus six years	Review and consider transfer to a Place of Deposit	Building plans and records of works are potentially of historical interest and where possible be kept and transferred to a place of deposit
Estates	CCTV		See ICO Code of Practice	Review and if no longer needed destroy	ICO Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf The length of retention must be determined by the purpose for which the CCTV has been deployed. The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.

Estates	Equipment monitoring and testing and maintenance work where asbestos is a factor	Completion of monitoring or test	40 years	Review and if no longer needed destroy	
Estates	Equipment monitoring and testing and maintenance work	Completion of monitoring or test	10 years	Review and if no longer needed destroy	
Estates	Inspection reports	End of lifetime of installation	Lifetime of installation	Review	
Estates	Leases	Termination of lease	12 years	Review and if no longer needed destroy	
Estates	Minor building works	Completion of work	retain for 6 years	Review and if no longer needed destroy	

Estates	Photographic collections of service locations and events and activities	Close of collection	Retain for not more than 20 years	Consider transfer to a place of deposit	The main reason for maintaining photographic collections is for historical legacy of the running and operation of an organisation. However, photographs may have subsidiary uses for legal enquiries.
Estates	Radioactive Waste	Creation	30 years	Review and if no longer needed destroy	
Estates	Sterilix Endoscopic Disinfector Daily Water Cycle Test, Purge Test, Nynhydrin Test	Date of test	11 years	Review and if no longer needed destroy	
Estates	Surveys	End of lifetime of installation or building	Lifetime of installation or building	Review and consider transfer to Place of Deposit	
Finance	Accounts	Close of financial year	3 years	Review and if no longer needed destroy	Includes all associated documentation and records for the purpose of audit as agreed by auditors

Finance	Benefactions	End of financial year	8 years	Review and consider transfer to Place of Deposit	These may already be in the financial accounts and may be captured in other records/reports or committee papers. Where benefactions endowment trust fund/legacies - permanent retention.
Finance	Debtor records cleared	Close of financial year	2 years	Review and if no longer needed destroy	
Finance	Debtor records not cleared	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Donations	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Expenses	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Final annual accounts report	Creation	Before 20 years	Transfer to place of deposit if not transferred with the board papers	Should be transferred to a place of deposit as soon as practically possible

Finance	Financial records of transactions	End of financial year	6 Years	Review and if no longer needed destroy	
Finance	Petty cash	End of financial year	2 Years	Review and if no longer needed destroy	
Finance	Private Finance initiative (PFI) files	End of PFI	Lifetime of PFI	Review and consider transfer to Place of Deposit	
Finance	Salaries paid to staff	Close of financial year	10 Years	Review and if no longer needed destroy	
Finance	Superannuation records	Close of financial year	10 Years	Review and if no longer needed destroy	

Legal, Complaints & information Rights	Complaints case file	Closure of incident (see Notes)	10 years	Review and if no longer needed destroy	http://www.nationalarchives.gov.uk/documents/information-management/sched_complaints.pdf The incident is not closed until all subsequent processes have ceased including litigation. The file must not be kept on the patient file. A separate file must always be maintained.
Legal, Complaints & information Rights	Fraud case files	Case closure	6 years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Freedom of Information (FOI) requests and responses and any associated correspondence	Closure of FOI request	3 years	Review and if no longer needed destroy	Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if not practical to keep a summary of the redactions.
Legal, Complaints & information Rights	FOI requests where there has been a subsequent appeal	Closure of appeal	6 years	Review and if no longer needed destroy	

Legal, Complaints & information Rights	Industrial relations including tribunal case records	Close of financial year	10 Years	Review and consider transfer to a Place of Deposit	Some organisations may record these as part of the staff record but in most cases they will form a distinct separate record either held by the staff member/manager or by the payroll team for processing.
Legal, Complaints & information Rights	Litigation records	Closure of case	10 years	Review and consider transfer to a Place of Deposit	
Legal, Complaints & information Rights	Patents / trademarks / copyright / intellectual property-	End of lifetime of patent or termination of licence/action	Lifetime of patent or 6 years from end of licence /action	Review and consider transfer to Place of Deposit	
Legal, Complaints & information Rights	Software licences	End of lifetime of software	Lifetime of software	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Subject Access Requests (SAR) and disclosure correspondence	Closure of SAR	3 Years	Review and if no longer needed destroy	

Legal, Complaints & information Rights	Subject access requests where there has been a subsequent appeal	Closure of appeal	6 Years	Review and if no longer needed destroy	